باسمه‌تعالی

کاربرگ شماره ۲

آگاهسازی حفاظتی حوزه فاوا

مطابق آئین نامهٔ جامع امنیت فاوای ودجا، دستورالعمل مهار تخلفات و شکست های حفاظتی و همچنین مصوبات کمیسیون امنیت و شورای فاوای دانشگاه، موارد ذیل در زمرهٔ شکست ها و تخلفات حوزه فاوایی می باشند:

- **اهم مصادیق شکست ها:**

۱. استفاده از رمزکننده های غیربومی (بیگانه) برای امور سازمانی؛
۲. ورود، نگهداری یا مبادله اطلاعات الکترونیکی (دیتا) دارای طبقه بندی خصوصاً سری و بالاتر در شبکه ها و کانال های ارتباطی (به استثناء شبکه های ویژه مجاز)؛
۳. استفاده از ذخیره سازهای شخصی برای نگهداری و جابجایی، چاپ دیتا و اطلاعات دارای طبقه بندی؛
۴. اتصال شبکه های سازمانی به شبکه های غیرسازمانی بدون کسب مجوز و اطمینان از سلامت امنیتی؛
۵. تولید، نگهداری و تبادل اطلاعات دارای طبقه بندی و سازمانی از طریق رایانه های متصل به اینترنت و شبکه های مرتبط با آن؛
۶. اتصال سخت افزار حاوی اطلاعات سازمانی به هرگونه شبکه غیرنظامی و اینترنت؛
۷. نقل و انتقال تجهیزات ارتباطی و امنیت فاوا دارای طبقه بندی به خارج از کشور بدون رعایت قوانین و مقررات ابلاغی؛
۸. آلوده شدن سامانه های دارای طبقه بندی به بدافزارها از جمله ویروس ها و کرم ها به علت قصور در پیش بینی و پیشگیری؛
۹. سرقت یا مفقودی رایانه همراه و هرگونه رسانه ذخیره ساز الکترونیکی سازمانی (فلش، لپ تاپ، انواع لوح فشرده، رایانه) حاوی اطلاعات دارای طبقه بندی و رمزکننده های بومی ن.م؛
۱۰. فروش رایانه ها و ابزارهای ذخیره ساز استفاده شده در ن.م به هر دلیل که امکان بازیابی اطلاعات آنها وجود دارد؛
۱۱. لزوم اخذ مجوز در ایجاد سایت های اینترنتی و ممنوعیت طرح و اخبار و اطلاعات در این سایت ها؛
۱۲. تعمیر تجهیزات دارای طبقه بندی فاوای ن.م در خارج از ن.م.

- **اهم مصادیق تخلفات:**

۱. رسیدگی نکردن به معایب و نواقص احصا شده در بازرسی های تامینی در مهلت مقرر؛
۲. بکارگیری تجهیزات فناوری اطلاعات بدون در نظر گرفتن مقررات و تائیدیه امنیتی؛
۳. عدم رعایت الزامات امنیتی در جابجایی اقلام فاوایی و تجهیزات ذخیره ساز به خارج از دانشگاه؛
۴. تجاری نمودن نرم افزارهای خاص ن.م و فروش آنها به خارج از ن.م بدون ملاحظات امنیتی و بکارگیری نرم افزارها بدون اخذ ارزیابی امنیتی از مراجع ذیصلاح؛
۵. رعایت نشدن الگوی استفاده از رمزکننده ها در شبکه‌های رایانه ای و سیستم‌های ارتباطی؛
۶. استفاده از شبکه‌های رایانه ای قبل از ارزیابی امنیت شبکه ها توسط مبادی ذیربط؛
۷. ورود و استفاده از تلفن همراه دوربین دار و هوشمند و سایر اقلام فاوایی و تجهیزات ذخیره ساز غیرمجاز (بدون اخذ مجوز) به داخل اماکن دارای طبقه بندی و یا اتصال آن‌ها به سایر سامانه های حاوی اطلاعات سازمانی و دارای طبقه بندی؛
۸. استفاده از صندوق پست الکترونیک جهت ارتباط و مبادله پیام با بیگانگان بدون تاییدیه ساحفا و بدون اخذ مجوز از فرماندهی؛
۹. راه اندازی شبکه اینترنت و یا استفاده از آن بدون رعایت ضوابط و مقررات مربوطه در ن.م؛
۱۰. عضویت و استفاده شخصی از شبکه‌های اجتماعی مجازی برای کارکنان ن.م بدون بکارگیری الزامات امنیتی اعلامی.

اینجانب ..... با کدملی ..... با عضویت ..... شاغل در مجتمع/معاونت ..... با مسئولیت ..... در جلسهٔ آگاهسازی مورخه / / حاضر و پیرامون محورهای تخلف و شکست فاوا، آگاهی لازم را کسب نموده و متعهد می‌گردم ضوابط و ملاحظات حفاظتی مصرحه را رعایت نمایم.

امضا توجیه شونده:

تاریخ: / /

امضا توجیه کننده:

تاریخ: / /

گفتنی است در صورت وقوع موارد اعلامی، فرآیند رسیدگی به شرح زیر دنبال می گردد:

۱) بررسی موارد تخلفات و شکست های فاوایی بر اساس دستورالعمل مهار تخلفات و شکست های فاوایی و ماتریس تخلفات؛

۲) تشکیل هیات بدوی (کمیته رسیدگی به تخلفات فاوایی) و بررسی موضوعات؛

۳) ارجاع تخلف به کمیسیون تخلفات فاوایی و صدور حکم توسط سردار ریاست محترم دانشگاه؛

٤) اعلام و ابلاغ احکام صادره به متخلفین و درج در پرونده.